1. Authorization Profile Storage

Claim 1 recites, in part, "a verification system . . . comprising a user storage, an authorization profile storage, and an audit log storage . . . ." As discussed in the specification, certain embodiments using such an authorization profile storage are afforded significant advantages:

> Additionally, information is stored into authorization profile storage 222, preferably by one who controls access to the system, such as a system administrator, a hotel cashier, or others, to specify which user may perform which transactions at what times and dates, etc. Thereafter, when a user attempts to access the system, his or her fingerprint is read by device 203, and compared with the known user storage 226, and the authorization profile storage 222 to determine whether to allow the particular user to perform the function requested. If so, the processor 216 then drives the access control signal 220, and logs the particular transaction, time, date, and identification information for the user. The identification of the user is verified continuously as long as the user is in contact with the biometric input device 203 .... *[I]f the user identifying information from the biometric device is matched with the user found in the known user storage 226, but the authorization profile storage 222 indicates that the particular user has requested something for which he or she is not authorized, then access is also denied*, and an audit log entry is also created in the audit log storage 224. This entry may include time, date, attempted transaction, and an indication of the user's identity, such as a name, a photographic image, or others." *Specification*, pages 15 through 16 (emphasis added).

Lemelson does not teach or suggest the features of independent Claim 1. Lemelson, in contrast to the present application, does not disclose, teach, or suggest a system utilizing an authorization profile storage as recited in the claims and explained, in relation to a specific embodiment, in the specification quoted above. In particular, the disclosure of Lemelson does not even mention (let alone teach or suggest) an authorization profile storage that allows for the storage of authorization information such as permissible dates, times, functions, or transactions for each user already known to a computer system. Further, Lemelson does not teach or suggest that such an authorization profile storage may be used to indicate whether a particular user has requested something (*e.g.*, by clicking a mouse) for which he or she is not authorized, and then to deny access to that user, if authorization does not exist.

Rather, Lemelson discloses a system in which a code signal or signals are generated that are used to identify a person entering and receiving data from a computer, which code signal is recorded for record purposes along with the information indicative of the information entered and/or received from the computer. *See* Abstract. Nowhere in Lemelson is there mention of an authorization profile storage as recited in the claims and explained above.

Because the cited art, taken alone or in any combination, does not teach or suggest the recited features of claim 1, and in particular, the features relating to an authorization profile storage, applicant respectfully submits that claim 1 is in condition for allowance. For at least the same reasons, all claims depending from claim1 are believed to be allowable as well, and Applicant therefore requests that those claims be allowed to pass to issue.

2. Audit Log Storage

Claim 1 recites, in part, "a verification system ... comprising a user storage, an authorization profile storage, and an audit log storage, *the audit log storage being configured to store user identification information from said biometric sensor in response to an unsuccessful transaction attempt and denial of access with said electronic system.*" As discussed in the specification, certain embodiments using such a verification system are afforded significant capabilities to detect internal fraud and unauthorized use:

> *If, at any time, a biometric reading is taken which does not match any user having a profile stored in the known user storage 226, access is denied and an audit log may be stored within the audit log storage 224 to provide a record of unsuccessful access attempts.* Such an audit log entry may include time, date, attempted transaction, *and a copy of the user identification information determined by the biometric device*, such as a scanned fingerprint image, a fingerprint minutia representation, or others. ... *Such an audit log affords a significant capability to detect internal fraud and other unauthorized use by persons known to the system, and indeed authorized perform some tasks, but not authorized for the task or function at the attempted time or date. Specification*, page 15 line 24 through page 16, line 10 (emphasis added).

Lemelson does not teach or suggest the features of independent claim 1. Lemelson, in contrast, discloses a system in which a code signal or signals are generated that are used to identify a person *entering and receiving data from a computer*, which code signal is recorded for record purposes along with the information indicative of the information *entered and/or received* from the computer. *See* Abstract. Thus, Lemelson allows for the storage of (a) a code signal to identify a person who has already gained access to the system, along with (b) information indicative of the information entered and/or received by that person who has already accessed the system. Although such a system may be useful to attribute data-entry errors to a person or person authorized to use, for instance, a cash register [*See* col. 11, lines 31-59], the system of Lemelson does not teach or suggest a system that allows for the storage of user identification information in response to an unsuccessful transaction attempt and denial of access with an electronic system, as recited in claim 1. In particular, there is no teaching in Lemelson to suggest that user identification information should be stored even if access is denied to a potential user in response to an unsuccessful transaction attempt.

At column 11, lines 31-59, Lemelson discloses that errors may be attributed to a person using a cash register because a code identifying the person is recorded with each cash-register transaction. Thus, if a user of the cash register performs an erroneous transaction, one may later attribute the error to the particular cash-register user. Again, as stated in the Abstract and confirmed by this cash-register example, the Lemelson system relates to the storage of information to identify a person who has already been allowed to enter and/or receive information from a computer (or cash register). The device recited in claim 1, however, provides even greater security measures because it is equipped with an authorization profile storage and an audit log storage that allow for the storage of user identification information in response to an *unsuccessful transaction attempt and denial of access* with an electronic system. In contrast to the system of Lemelson, Applicant's system therefore allows for (a) the denial of access if a transaction is not authorized and (b) the storage of user identification information in response to the unsuccessful transaction attempt and denial of access. So, if a cash-register were utilizing the recited features of claim 1, a cash-register user could be denied access (via the authorization profile storage) if he even attempted to enter an erroneous transaction – also, if he attempted such

a transaction, his user identification information (such as a fingerprint) could be stored in an audit log storage (even though he was denied access) so as to form a record of the unsuccessful transaction attempt. Thus, in contrast to the Lemelson system, certain cash-register errors could be prevented altogether (via a denial of access), and those even *attempting* to enter an erroneous transaction could be "finger-printed." Unlike the system of Lemelson, which allows a person to review and attribute erroneous transactions to a certain user *after they have already been completed and the damage is done*, the features of Applicant's invention both prevent and track fraud. These features, which are nowhere taught or even suggested by the cited art, act as a powerful fraud-deterrent for a variety of electronic systems

Because the cited art, taken alone or in any combination, does not teach or suggest the recited features of claim 1, and in particular, the features relating to an audit log storage being configured to store user identification information in response to an unsuccessful transaction attempt and denial of access with an electronic system, Applicant respectfully submits that claim 1 is in condition for allowance. For at least the same reasons, all claims depending from claim 1 are believed to be allowable as well, and Applicant therefore requests that those claims be allowed to pass to issue.

C. New Claims 49-60

New claims 49-60 are allowable for at least the reasons their parent claim 1 is allowable. Further, claims 56-59, relating to a substance detection sensor, are patentably distinct over the cited art as well – including Matchett, Lemelson, and Axelrod. Matchett, taken alone or in combination with Lemelson and Axelrod, does not teach or suggest the recited substance detection sensor. Matchett makes no mention of such a sensor, and the earlier-cited portions of Axelrod simply disclose that an auxiliary data input may include a breathalyzer so that additional data may be appended to a record. This does not amount to a teaching or suggestion of the features recited Applicant's claims, and for this reason as well, claims 56-59 are believed to be in condition for allowance.

D. New Claim 61

New independent claim 61, directed to a pointing device wherein the toe of a user's foot is in proximity to and readable by a biometric sensor, is believed to be in condition for allowance for at least the reasons claim 1 is allowable, as discussed in detail above.

E. New Claims 62-66

New claims 62-66 relate to a pointing device including a upper section moveably connected to a base such that a trackball is positionable adjacent a left or right side. These claims are believed to be allowable because such features are nowhere taught or suggested in the cited art, taken alone or in combination. Further, these claims are believed to be allowable for at least the reasons claim 25 of the parent-application to this application was deemed allowable by the Office.

F. New Claims 67-70

New claims 67-70 relate to a computer verification system including an audit log storage being configured to store user identification information from a biometric sensor in response to an unsuccessful transaction attempt and denial of access with an electronic system. These claims are in condition for allowance for at least the reasons claim 1 is allowable, as discussed in detail above.

G. New Claims 71-78

New claims 71-78 relate to a method for verifying a user of an electronic system and include the step of storing identification information and attempted transaction information of a user in an audit log storage if the user is not authorized to perform a selection and is denied access to the electronic system. These claims are allowable for at least the reasons claim 1 is allowable, as discussed in detail above. Further, claims 75-78, relating to a substance detection

sensor, are allowable because the features recited therein are not taught or suggested by the cited art, taken alone or in combination.

H. New Claims 79-81

New claims 79-81 relate to a verification system and is allowable for at least the reasons as discussed in detail above. In particular, none of the cited art, taken alone or in combination, teaches or suggests the recited user storage, authorization profile storage, and audit log storage.

CONCLUSION

Applicant believes that the foregoing remarks fully respond to all outstanding matters for this application. Applicant respectfully submits that the rejection of all the claims should be withdrawn, and that the claims should be passed to issue

Should the Examiner desire to sustain any of the rejections discussed in relation to this preliminary amendment, the courtesy of a telephonic conference between the Examiner and the undersigned attorney at 512-418-3018 is respectfully requested.

Respectfully submitted,

Michael C. Barrett

Michael C. Barrett
Reg. No. 44,523
Attorney for Applicant

FULBRIGHT & JAWORSKI L.L.P.
600 Congress Avenue, Suite 1900
Austin, Texas 78701
(512) 418-3000

Date: May 30, 2000